基于多素数和参数替换的改进 RSA 算法研究 *

周金治 [a†]，高　磊 [b]

(西南科技大学 a. 信息工程学院; b. 特殊环境机器人技术四川省重点实验室，四川 绵阳 621010)

摘　要：为了提高 RSA 公钥算法在消息加密过程中的安全性，在深入分析传统 RSA 算法的基础上，对其进行一些改进性研究，提出了一种比传统 RSA 算法更加有效的方法优化其安全性。在将传统 RSA 改进为四素数 RSA 的基础上，再运用数学变换进行参数替换，消除了在公钥中对传输两个随机素数的乘积 n 的需要，引入了一个新的参数 x 代替原参数 n。针对改进后的算法在运算效率方面的不足，采用中国剩余定理(Chinese remainder theorem，CRT)优化大数模幂运算。实验结果证实了改进算法的可行性，为通过公钥加密消息发送和接收提供了更安全的路径；同时，对改进算法与传统 RSA 和四素数 RSA 算法的解密(签名)时间进行比较分析。实验结果表明改进后的算法对消息发送方和接收方之间签名效率也有一定程度的优化。

关键词：RSA 算法；数据加密；参数替换；中国剩余定理；公钥；签名效率

中图分类号：TP312　　doi: 10.3969/j.issn.1001-3695.2017.09.0879

Research on improved RSA algorithm based on multi-prime number and parameter substitution

Zhou Jinzhi[a†], Gao Lei[b]

(*a. School of Information Engineering*, *b. Robot Technology for Special Environment Key Laboratory of Sichuan Province*, *Southwest University of Science & Technology*, *Mianyang Sichuan* 621010, *China*)

Abstract: In order to achieve greater safety in RSA encryption algorithm in the data encryption process, this paper made some improvements based on in-depth analysis on the traditional RSA algorithm. It put forward a more secure method with changing traditional double primes into four primes in the traditional RSA algorithm and eliminating the requirement for transferring the product n of two random primes in public key on the basis of parameter substitution. Instead, this paper replaced the original parameter n to a new introduced parameter x. In order to boost the efficiency in the introduced algorithm, this paper used the CRT(Chinese remainder theorem) to expedite the exponentiation of large numbers. The results demonstrates the feasibility of the improved algorithm, provides a safer path for messages transmission through public key encryption. At the same time, this paper carried out a comparative analysis of encryption and decryption time among the improved algorithm and the traditional double primes and four primes RSA algorithms. The results shows that the improved algorithm to a certain degree enhanced the encryption and decryption efficiency between the message sender and receiver.

Key Words: RSA algorithm; data encryption; parameter substitution; the Chinese remainder theorem; public key; decryption efficiency

0　引言

随着信息通信技术在互联网时代的不断发展，信息安全问题日益受到人们的广泛关注，以密码学为基础的信息安全技术也得到了飞速的发展。数据加密技术根据密钥的类型发展出了两种不同的密码体制，分别是对称的密码密钥体制（symmetric-key cryptosystem）和非对称密钥密码体制（asymmetric-key cryptosystem）。其中，非对称密钥密码体制涉及使用两个不同但相关的密钥，即公钥和私钥[1]。明文通过公钥被转换成密文。这个过程称为加密，由发送方执行。另一方面，通过使用接收方的私钥来执行密码文本的解码。这个过程称为解密，由接收者执行。为了保持私钥的机密性，公开密钥公开给公众。公钥用于身份验证，以确保消息来自预定发送者。只有接收方的私钥才能解密源于发送方的密码文本。因为公钥的知识不足以解密密文，所以消息的通信可以以安全的方式进行。

传统 RSA 算法容易遭受到选择密文攻击、出错攻击、连分数攻击和对模数 *n* 的分解攻击[2]。关于如何改进 RSA 算法以提高其安全性，文献[3,4]提出了一种新的算法概念和为加快整个

基金项目：特殊环境机器人技术四川省重点实验室基金资助项目（13ZXTK07）

作者简介：周金治，男（通信作者），副教授，硕士，主要研究方向为计算机网络、传感网技术应用、智能家居、语音识别等（homehawk@263.net）；高磊（1993-），男，硕士研究生，主要研究方向为网络通信、信息安全等.

网络的数据交换过程中 RSA 算法实现的改进形式，通过在公钥和私钥的构成中使用额外的第三素数的方法增加参数 n 的因式分解复杂性，但容易受到选择密文攻击。文献[5]提出了一种消除参数 n 的改进 RSA 密码体制，但只给出了一个特例进行说明，缺乏基于实验的科学论证，结论不具备说服力。文献[6]提出了一种基于参数 n 的改进 RSA 算法，通过使用四个素数优化现有的 RSA 算法，这种方法依然可以通过因数分解的方法得到密钥，从而对消息进行攻击。

在标准 RSA 算法中，公钥和私钥这两者之间存在一个数学关系，这一事实为密码攻击者发现与破解密钥之间的关系进而成功地派生出私钥提供了可能性。本文应用一种数学变换替换参数 n，增加了攻击者确定这个因素的困难度，从而优化 RSA 算法的安全性能。

1　RSA 算法及相关问题分析

1.1　算法原理

非对称加密算法中最著名的是由美国 MIT 的 Rivest 等人[7]于 1978 年发表的 RSA 算法，它也是目前应用最为广泛的公钥加密算法，现在被国际标准化组织（International Organization for Standardization，ISO）推荐为公钥数据加密标准。它是一种非对称密钥密码体制，涉及到将公共密钥和私有密钥分配给发送方和接收方来加密和解密消息。在加/解密时使用的是两种不同的密钥，即加密密钥与解密密钥。其安全性是基于数论和计算复杂性理论，两个大素数乘积的计算是十分容易的，但是想要很快将两个大素数的乘积分解，求出它的因子在计算上是困难的，至今还没有一种方法能够很好的将其破解。利用 RSA 公钥加密算法对消息加密后，消息的安全性主要就是依赖于大整数因式分解的复杂性[8]。RSA 公钥加密算法包含密钥生成、消息加密、消息解密三个步骤，下面给出算法描述。

1.1.1 RSA 密钥生成

任意选取两个不相干的大素数 p 和 q 将其保密存储起来；

计算 $n=pq$ 和欧拉函数 $\phi(n)=(p-1)(q-1)$；

随机地选取一个正整数 e，使其满足 $1<e<\phi(n)$，并且要求 e 和 $\phi(n)$ 的最大公约数 $GCD(e,\ \phi(n))=1$，那么公开的加密密钥，即公钥为(e，n)；

计算解密密钥 d，使其满足 $0<d<\phi(n)$，且 $ed\equiv 1(mod\ \phi(n))$，即私钥为 $(d,\ n)$。

1.1.2 消息加密

消息发送方使用下面方式对明文 M 进行加密：

$$C=M^e mod(n)$$

1.1.3 消息解密

消息接收方使用下面方式对密文 C 进行解密：

$$M=C^d mod(n)$$

其中：M 代表需要加密的明文；C 代表加密后的密文；e 代表加密时候的密钥；d 代表解密时候的密钥；n 代表模数。

1.2　可优化性分析

RSA 从发表到现在已有近四十年的时间，其间经历了各种攻击的考验，是最典型也是被研究得最成熟的，至今仍是公钥密码学最优秀的算法之一。虽然 RSA 算法的安全性是建立在大整数的因式分解基础之上，但是到目前还没有从理论上证明破译 RSA 的难度等价于大整数因式分解的难度，即从理论上掌握 RSA 的加密性能还无法实现。而且对于大量数据的加/解密，RSA 算法的可优化之处分为算法安全性和运算效率两个方面，下面逐一分析。

1.2.1 安全性分析

本文就针对参数 n 的攻击进行算法安全性分析。

（1）模数 n 的因式分解

在公开密钥中，密码攻击者可以利用伪造的签名对模数 n 进行分解，那么则有可能计算出 $\phi(n)=(p-1)(q-1)$。这样，解密密钥就可以求出，从而整个 RSA 公钥算法就被破译了。例如，密码攻击者可以通过下述方法对 n 进行因子分解：

(a)根据 $\phi(n)=(p-1)(q-1)=n-(p+q)+1$ 和 $n=pq$ 可以求得 $p+q=\phi(n)+1$；

(b) $(p+q)^2=p^2+2pq+q^2=(p-q)^2+4pq$ 可以求得 $p-q=\sqrt{(p+q)^2-4n}$；

(c) 根据 $p=((p+q)+(p-q))/2$ 求出 p；

(d)再由 $n=pq$ 求出 q。

至此，攻击者完成了对参数 n 的因子分解，由此就可能破解 RSA 密码系统。

（2）RSA 的选择密文攻击

由于 n 是通过公钥传输的，所以攻击者可以使用公钥加密明文，然后通过点击和试用找出其影响因素。如果任何密文与之匹配，攻击者就可以了解秘密消息，从而降低 RSA 算法的安全系数。选择密文攻击是指密码攻击者事先选择不同的密文，让被攻击的算法解密，利用未知的密钥取得与之对应的明文，由此推算出私钥或模数，进而获得自己想要的明文，是针对 RSA 等公钥算法最常用的攻击方法[9]。例如，如果攻击者想破译消息 x 获取其签名，可以事先虚构两个合法的消息 x_1 和 x_2，使得 $x\equiv(x_1x_2)(mod n)$，并骗取用户对 $x1$ 和 $x2$ 的签名 $S_1=x_1^d(\bmod n)$ 和 $S_2=x_2^d(\bmod n)$，就可以计算出 x 的签名：

$$S=x^d=(((x_1x_2)(\bmod n))^d)(\bmod n)$$

$$=((x_1^d \bmod n)(x_2^d \bmod n))\bmod n$$

$$=(S_1S_2)(\bmod n)。$$

1.2.2 效率分析

RSA 公钥算法发展的最大瓶颈是大整数的模幂运算，目前 RSA 密码系统的模数 n 已经可以到 2 048 位，其算法效率必然会受到如此巨大的模数的影响。关于如何加快数据传输过程中的 RSA 算法的实现，目前有很多不同的算法被提出，比如 Sliding window、modular repeat squaring 算法、基于乘同余对称

特性和指数 2k 次方组合优化算法等[10]。文献[4]和[11]分别提出了一种在 RSA 算法中对关键参数的离线存储和密钥脱机生成的方法，在一定程度上优化算法的运算效率，但程度很低。文献[12]使用四个素数因子，计算了一对公钥和私钥中的两个自然数，这两个自然数增加了密码体制的安全性，然而并没有从实验角度证明改进后算法的可行性与正确性。文献[13]综合使用对称密码算法 AES-128 和非对称密码算法 RSA。AES-128 算法在消息传递过程中保持数据消息的机密性和完整性，RSA 算法来处理消息的认证性和不可否认性，在效率上也有比较优秀的表现。本文从算法运算效率的角度出发，将 CRT 融入四素数 RSA 算法，再将其运用到数字签名中。

2 RSA 算法优化

2.1 基于四素数的 RSA

对于相同的密钥位数，四素数 RSA 算法比传统 RSA 算法所要求产生的随机素数要小，还能够减少密钥生成的运算量。另外，素数因子越小，大整数因式分解就越便利。但是素数使用得越多，RSA 算法的安全强度会越低。本文对比传统 RSA 算法，采用选取四个随机大素数的方法，其描述简述如下。

2.1.1 密钥生成

随机产生四个不同的大素数 p、q、r 和 s，计算：

$$n = pqrs \text{ 和 } \phi(n) = (p-1)(q-1)(r-1)(s-1) \text{。}$$

2.1.2 消息加密

$$C = M^e mod(n)$$

2.1.3 消息解密

$$M = C^d mod(n)$$

2.2 中国剩余定理优化运算效率

中国剩余定理(Chinese remainder theorem, CRT)是中国古代求解一次同余式组的方法，也是初等数论中重要的基本定理之一。其内容为：设 $m_1, m_2, \ldots, m_k$ 是 k 个两两互素的正整数，$a_1, a_2, \ldots, a_k$ 是 k 个任意整数，$M = m_1 m_2 \ldots m_k$，$i = 1, 2, \cdots, k$，则同余数组 $x = a_i \bmod m_i$ 唯一解的表达式为 $x = \sum_{i=1}^{k} a_i M_i b_i (\bmod M)$。其中，$b_i M_i = 1 \bmod m_i$，$M_i = M / m_i$，$i = 1, 2, \cdots, k$。

假设明文为 M，密文为 C，下面给出在 RSA 算法中应用中国剩余定理的具体过程：

计算 M 的剩余

$$\begin{pmatrix} M_p = C_p^{d_p} \bmod p \\ M_q = C_q^{d_q} \bmod q \\ M_r = C_r^{d_r} \bmod r \\ M_s = C_s^{d_s} \bmod s \end{pmatrix}$$

其中：$C_p = C \bmod p$，$C_q = C \bmod q$，$C_r = C \bmod r$，$C_s = C \bmod s$；$d_p = d \bmod (p-1)$，$d_q = d \bmod (q-1)$，$d_r = d \bmod (r-1)$，$d_s = d \bmod (s-1)$。

根据中国剩余定理，可得

$$\begin{pmatrix} M \equiv M_p \bmod p \\ M \equiv M_q \bmod q \\ M \equiv M_r \bmod r \\ M \equiv M_s \bmod s \end{pmatrix}$$

可解得

$M = (M_p (qrs)^{p-1} + M_q (prs)^{q-1} + M_r (pqs)^{r-1} + M_s (pqr)^{s-1}) \bmod n$，即为原明文 M。

由上述过程可见，该定理的优势在于能把大整数的模幂运算转换成相对较小的数的模幂运算，在 RSA 算法应用 CRT，能够降低消息解密时的运算量和复杂度。

2.3 参数 n 的替换优化安全性

在传统 RSA 算法中，两个密钥都包含参数 n，这可以被分解为两个大素数。如果密码攻击者猜出 n 的因素，就很容易得到私钥。为了克服 1.2.1 节所分析的针对参数 n 攻击的这一弱点，本文在四素数 CRT-RSA 算法基础上，再试图消除两个密钥中 n 的分布，用一种改变原模（两个素数乘积）的方法，即引入了一个新的参数 x 代替原参数 n，使攻击者难以通过针对 n 进行攻击。更改的模数值将被公开声明，这可能是假值。即使攻击者因式分解这种新的模值，他无法找到原来的解密密钥。无法找到原始解密密钥，分解是毫无价值的。至此，结合 2.1 和 2.2 节所述的优化方法，改进后的 RSA 算法同样包含三个步骤，即生成替换参数 n 的密钥、消息加密和消息解密。

2.3.1 密钥生成

选定四个任意的大素数 p、q、r 和 s，计算 $n = pqrs$ 和欧拉函数 $\phi(n) = (p-1)(q-1)(r-1)(s-1)$。

随机地选取一个正整数 e，使其满足 $\sqrt{n} < e < \phi(n)$，并且要求 e 和 $\phi(n)$的最大公约数 $GCD(e, \phi(n)) = 1$。

计算 x（用来代替 n），计算步骤如下：

如果 $q < p$，则定义 x：$(n-p) < x < n$，$GCD\ (x, n) = 1$；

如果 $q > p$，则定义 x：$(n-q) < x < n$，$GCD\ (x, n) = 1$。

计算解密密钥 d，而且 $ed \equiv 1 (mod\ \phi(n))$。此时，公钥为 (e, x)，私钥为 (d, x)。

2.3.2 消息加密

消息发送方使用 (e, x) 对明文 M 进行加密：

$$C = M^e \bmod (x)$$

2.3.3 消息解密

消息接收方使用 (d, x) 对密文 C 进行解密：

$$M = C^d \bmod (x)$$

改进 RSA 算法流程如图 1 所示。

3 实验结果及分析

实验在 i5-2450M CPU，6 GB 内存和 Windows 64 位系统下选用 MATLAB R2016a 工具进行，在算法实现关键步骤中，素性检测采用最成熟的 Robin-Miller 检测法，用中国剩余定理 CRT 的算法来实现大整数模取幂的运算，求解解密密钥 d 时的

模逆运算采用费马小定理：a 是整数，p 是素数，且 a 和 p 互素，即 $GCD(a,p)=1$，恒有 $a^{p-1} \bmod p=1$。进而 $a^{-1}=a^{p-2} \bmod p$，将模逆运算用多项式运算来替代，在原算法基础上进一步优化运算的效率。通过对比文献[14]中散列函数 MD5、SHA-160，SHA-256 和 SHA-512，本实验中采用 SHA512。

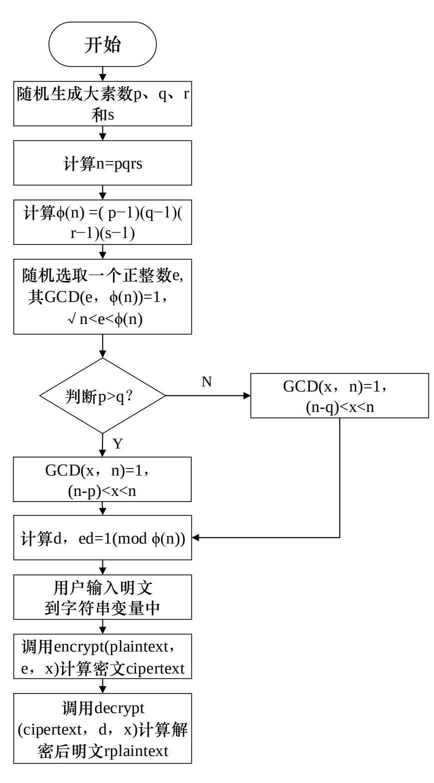


图 1　改进 RSA 算法流程

本实验中，将传统 RSA 算法改进为融入 CRT 的四素数 RSA 算法，并用一个新的参数 x 代替原本公开的 n 进行了保密处理，通过生成两组随机素数进行对比，加密后的密文无法被识别，很好地保护消息的安全性，证实这种改进 RSA 算法能取得良好加/解密效果。

改进 RSA 算法效果如图 2 所示。



图 2　改进 RSA 算法效果

本文用 Robin-Miller 算法分别生成 256 bit、512 bit 和 1 024 bit 素数，然后让传统 RSA、传统四素数算法和改进后的算法分别在位大小变化的情况下进行测试。

3.1　密钥生成时间对比

算法的密钥生成时间如表 1 所示。由表中三种算法生成密钥所耗时间对比可知：256 bit 时改进算法的密钥生成速度是传统 RSA 算法 1.68 倍；512 bit 时为 1.73 倍；1 024 bit 时达到 1.81 倍。虽然改进算法相比传统四素数 RSA 算法耗时有所增加，但比起改进算法在安全性方面所做贡献而言微不足道，本文将在 3.3 节加以分析。为了更加直观地观察两种算法效率，将两种算法所耗时间放在图 3 中进行对比（下同）。

表 1　算法生成密钥耗时情况

时间/ms	传统 RSA 算法生成密钥	四素数 RSA 算法生成密钥	改进 RSA 算法生成密钥
256 bit	3 128	1 784	1 855
512 bit	9 319	5 235	5 368
1024 bit	75 701	39 472	41 736

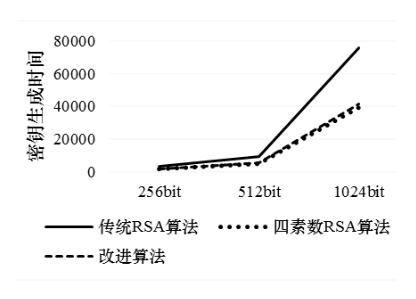


图 3　算法密钥生成时间对比

3.2　算法解密时间对比

三种算法的解密时间如表 2 所示。对比所耗时间可知，256 bit 情况下，改进后的算法解密速度达到了传统 RSA 算法的 5.88 倍；512 bit 时为 9.85 倍，与理论值 10.86 倍接近；1 024 bit 时达到 10 倍。对比改进算法与四素数 RSA 算法，其速度也有大幅度提升。算法解密时间对比如图 4 所示。

表 2　算法解密耗时情况

时间/ms	传统 RSA 算法解密	四素数 RSA 算法解密	改进 RSA 算法解密
256 bit	459	201	78
512 bit	3 261	1 020	331
1024 bit	24 783	8 182	2 469

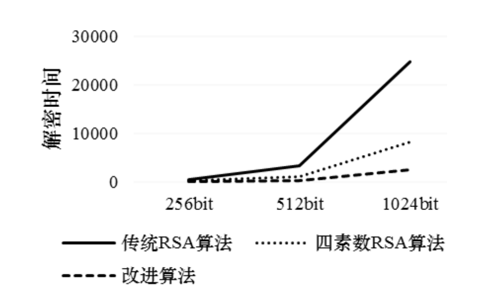


图 4　算法解密时间对比

3.3 Brute-force 攻击时间对比

为了对大整数 n 因式分解，采用基于椭圆曲线的分解算法（ECM）和一般数域筛法（GNFS）相结合的方法。ECM 通常用于小整数因式分解，而 GNFS 能够分解位数大于 100 的大整数。实验分别对对三种算法采用暴力攻击（brute-force），所耗时间如表 3 所示。从表中可以看出，生成 16 bit 素数情况下，传统算法暴力分解参数 n（改进算法中替换为 x）需要 78.676s，四素数 RSA 算法需要 126.498 s，而改进算法中则需要 243.95 s。改进算法被暴力分解的所需时间是传统 RSA 算法的 3.1 倍，是四素数 RSA 算法的 1.93 倍。可以推断，当比特更高时，传统 RSA 算法与改进算法耗时的差距会更大。由此可见，改进后的算法有助于克服 RSA 中参数 n 易被因式分解攻击的弱点。Brute-force 攻击时间对比如图 5 所示。

表 3　Brute-force 攻击耗时情况

时间/s	传统 RSA 算法 Brute-force	四素数 RSA 算法 Brute-force	改进算法 Brute-force
8 bit	1.564	6.383	13.894
10 bit	6.151	19.578	35.204
16 bit	78.676	126.498	243.95

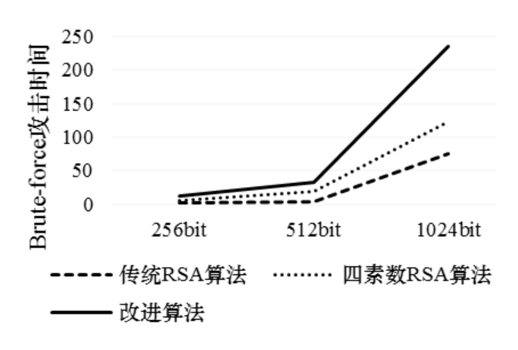


图 5　Brute-force 攻击时间对比

4　结束语

针对 RSA 公钥算法攻击最直接的方法是对模数 n 进行素因子分解，本文在讨论算法可优化性的基础上，提出了一种改进的 RSA 公钥算法，在四素数算法中融入中国剩余定理，并消除原始 RSA 算法中的参数 n，添加一个新的参数 x 替换私有和公钥中的 n，并通过实验验证了提出的 RSA 算法的有效性。同时，针对生成的 256 bit、512 bit 和 1 024 bit 素数分别用标准 RSA、四素数 RSA 算法和改进 RSA 算法进行实验，记录算法的密钥生成时间和解密所耗的时间。实验结果显示，改进 RSA 算法的签名时间大幅降低，提高了算法签名的效率，比传统 RSA 算法具有一定的优势。用 Brute-force 攻击 8 bit、10 bit 和 16 bit 时的参数 n，对比三种算法的被攻破时间，改进算法所消耗的时间显然长于其他两种算法。结果表明改进算法在提高签名速度的同时还提高了算法的安全性，证明了基于多素数和替换参数 n 的改进 RSA 算法的优越性和实用性。在今后的实验和应用中使用该改进算法提高 RSA 系统的安全系数和运算速度，使 RSA 算法得到进一步发展。

参考文献：

[1] Chhabra A, Mathur S. Modified RSA algorithm: a secure approach[C]//Proc of International Conference on Computational Intelligence and Communication Networks. Gwalior, India: IEEE Press, 2011: 545-548.

[2] 肖振久，胡驰，陈虹. 四素数 RSA 数字签名算法的研究与实现[J]. 计算机应用, 2013, 33(5): 1376-1377.

[3] Arora S, Pooja. Enhancing cryptographic security using novel approach based on enhanced-RSA and elamal: analysis and comparison[J].International Journal of Computer Applications, 2015, 112 (13): 35-39.

[4] Al-Hamami A H, Aldariseh I A. Enhanced method for RSA cryptosystem algorithm[C]//Advanced Computer Science Applications and Technologies. Kuala Lumpur, Malaysia: IEEE Press, 2013: 402-408.

[5] Sahu J, Singh V, Sahu V, et al. An enhanced version of RSA to increase the security[J]. Journal of Network Communications and Emerging Technologies, 2017, 7(4): 1-4.

[6] Thangavel M, Varalakshmi P, Murrali M, et al. Comment on an enhanced and secured RSA key generation scheme (ESRKGS)[J]. Journal of Information Security & Applications, 2015, 20 (C): 3-10.

[7] Rivest R, Shamir A, Aldeman L. A method for obtaining digital signatures and public-key cryptosystems[J]. Communications of the ACM, 1978, 21(2): 120-126.

[8] 冯登国，赵险峰. 信息安全技术概论[M]. 北京：电子工业出版社, 2012: 30-32.

[9] 李家兰. RSA 算法的攻击方法研究[J]. 科技视界, 2015(2): 50.

[10] 何俊杰，焦淑云，祁传达. 一个基于身份的签密方案的分析与改进[J]. 计算机应用研究, 2013, 30(3): 913-916,920.

[11] Nagar S A, Alshamma S. High speed implementation of RSA algorithm with modified keys exchange[C]//Proc of the 6th International Conference on Sciences of Electronics, Technologies of Information and Telecommunications.Sousse, Tunisia: IEEE Press, 2012: 639-642.

[12] Mahaveerakannan R, Dhas C S G. Customized RSA public key cryptosystem using digital signature of secure data transfer natural 22 number algorithm[J]. International Journal of Computer Technology & Applications, 2016, 9(5): 2627-2632.

[13] Siregar H, Junaeti E, Hayatno T. Implementation of digital

signature using aes and rsa algorithms as a security in disposition system af letter[J].Materials Science and Engineering, 2017, 180(1):12-55.

[14] Mansour A H. Encryption and decryption analysis of the RSA digital signature based on MD5 and SHA hash functions using strong prime[J]. Journal of Soft Computing and Decision Support Systems, 2017, 4(1): 7-15.